46.4 Annexure-D

Functional and Technical Specifications Compliance

# (Note: Fields with * are Security related)	Compliance to Technical Specifications	Must Have /Nice to Have	Compliance (Y/N)	Bidder to mention (Available / Work Around / Not Available	Bidder's comment on how they comply to the requirement.	Remarks
A	**General**					
i.	The proposed HCI should support at least two leading hypervisors.	Must have				
ii.	The HCI solution should contain a simplified provisioning and administration of virtual networking through a centralised network management software	Must have				
iii.	The solution should provide a tool based physical-to-virtual conversion to migrate existing physical workloads to the virtual platform with minimal disruption	Must have				
iv.	There should be GPU (Ex. NVIDIA TESLA v100 32 GB or Equivalent) based infrastructure available for high performance data computation.	Must have				
v.	The solution should provide zero down time, zero-data loss in case of disk, host, network or Rack power failure, continuous availability against physical host failures	Must have				
vi.	The solution should provide hyper-converged software that allows delivery of enterprise-class storage services using latest x86 server infrastructure without dependence on a separate Storage Area Network & associated component such as SAN Switches & Host Bus Adapters (HBA).	Must have				
vii.	The proposed HCI software solution and licenses should be PERPETUAL in nature and should have NO dependency on underlying hardware	Must have				

viii.	The Bidder should mention resource requirements of all necessary management components (including any storage controller, VM requirements on each host) in the proposal for the solution to be deployed	Must have				
ix.	The solution should provide support for heterogeneous guest operating systems such as Windows (Desktop & Server OS) and Linux (at least Red Hat, SUSE, Ubuntu and CentOS) and Solaris x86 etc.	Must have				
x.	The solution should provide unified and centralized software defined datacentre platform that brings together compute, storage, networking and security virtualization into a natively integrated stack to deliver enterprise ready private cloud infrastructure.	Must have				
xi.	The solution should include unique lifecycle management services that automate day 0 to day 2 operations, from bring up to configuration, resources provisioning and patching/upgrades.	Must have				
xii.	The solution should provide the network virtualization platform for software defined datacentre, delivering the operational model of a virtual machine for entire networks including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment.	Must have				
xiii.	The bidder should be a single point of contact for the entire project (Software Stack, Hardware, Network components and all the licenses and support services.	Must have				
xiv.	Solution should provide automation and orchestration solution for automated delivery of IaaS, PaaS, XaaS/ SaaS services so that when VM/app is created it should automatically get the required virtualized compute, storage, switching, routing, firewall, load balancing services without any manual intervention. All compute, network, storage, security, load balancing policies must follow the life cycle of VM	Must have				

	and movement within and across private cloud.						
xv*	Single Management Console: It should have One Click Infrastructure Management, One Click Operational insights, One Click Capacity Planning and One Click Security management. (i) It should support Backup, Clusters in private cloud, replications, backup node and all these capabilities can be configured and managed through this single management console. (ii) Central dashboard should enable multiple clusters to be monitored and managed including consolidated alerts, available storage, performance in terms of both bandwidth and IOPS, and more.		Must have				
xvi.	Solution should support multiple OEM/hardware choice.		Must have				
xvii.	The services can be deployed as a group of interconnected VMs in the private cloud with specific deployment dependencies and, optionally, some location, affinity, and elasticity requirements.		Must have				
xviii.	Multitier service deployment should support virtual networks, virtual storage etc.		Must have				
B	**Compute**						
1	**Rack Server Specification**						
i.	Processors	Rack Server should have latest generation Processors	Must have				
ii.	Chipset	Latest chipset compatible with the offered processors	Must have				
iii.	Internal Storage	As applicable to installed Hypervisor	Must have				
iv.	Memory	Should have at least 24 DIMM slots per server and support up to 1.5TB of DDR4 memory or equivalent	Must have				
v.	Network	Server should have 4 port 10 Gbps SFP+ Card	Must have				

vi.	PCIe Slots	Minimum 4 PCIe Generation 3.0 slots or as applicable	Must have				
vii.	Pre-failure Alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	Must have				
viii.	Configuration & Management	Real-time hardware performance monitoring & alerting	Must have				
ix.*	Server Security	Should have built in server security & recovery tools	Must have				
2	**Minimum Hardware Specification for Node**						
i.	2U Rack Mountable or lower		Must have				
ii.	CPU - Minimum Two x 24 core with latest series Processor		Must have				
iii.	Memory - Minimum 256 GB DDR4 expandable to 1TB DDR4		Must have				
iv.	Redundant hot plug power supplies		Must have				
v.	Redundant hot plug fans		Must have				
vi.	Each server must have additional free slots for RAM and HDD in future use		Must have				
vii.	Solution should have 2x disk upgrade capacity of the proposed solution current capacity.		Must have				
3	The solution should be scalable in a non-disruptive manner by adding additional nodes to the cluster at a later point of time without having to power down any nodes		Must have				
4	Scale hyper converged node (compute + storage), compute-intensive or storage intensive independent of each other should be supported		Must have				
5	In the event of a node failure, virtual machines should automatically run on another node		Must have				

6	The solution should provide the ability to scale-up (by adding more disks to existing nodes) or scale-out (by adding more nodes to the cluster) in terms of storage and compute	Must have				
7	The proposed solution must be able to sustain one node failure and it should be in no way affect/degrade the production services & usable resources and applications	Must have				
8	The solution should provide the ability to rapidly on-board new hosts to the data centre platform by automatically deploying reference configurations including networking settings	Must have				
9	The solution should provide guidance on right-sizing, resource consumption, risks and future issues that are unique to every data centre environment	Nice to have				
10	The solution should provide the ability to hot-add CPU and memory and hot-plug disks and NICs (provided the same is supported by the guest operating system). This should be via GUI.	Must have				
11	The information on the resources in use by any virtual domain needs to be available at any given time. This information should include both the physical and management resources associated with the virtual domain(s)	Must have				
12	The solution must support virtual machine formats/type compatible with cloud systems like Amazon, Google, Azure, VMWare, CISCO and Red Hat etc.	Must have				
13	No service interruption with up to 2 Node/server failure	Must have				
14	The solution should provide ability to logically group instances for applications that require low network latency and/or high network throughput.	Must have				
15	Bidder should make sure that compute instances architected in such way to avoid any outage or downtime when Bidder performing any maintenance activity	Must have				
16	Compute instances must provide anti-virus protection.	Nice to have				

17	Bidder should ensure that if at any point, compute instance fails it should automatically start on healthy physical host.	Must have				
C	**Network and Security**					
1	**General**					
i.	Dynamic routing between virtual networks	Must have				
ii.	Stateful firewalling distributed across the network	Must have				
iii.*	Firewall capability for East-West Traffic Protection	Must have				
iv.	The solution should provide a virtual load balancer to scale application delivery	Must have				
v.	Each Hyper Converged node should provide minimum 4 x 10Gbps SFP+	Must have				
vi.	The solution should provide a software defined and virtualized networking model that allows placement of virtual workloads on segments of networks that are isolated from each other without dependence on the underlying physical networking infrastructure configuration	Must have				
vii.	The solution should provide simplified GUI based configuration of switching capabilities such as RSPAN, ERSPAN, IPFIX, SNMP v3 & QoS across the cluster with the ability to backup & restore network configurations	Must have				
viii.	Backup and Restore networking configurations with rollback and recovery	Must have				
ix.	Proposed solution should be able to integrate Internal Network within VM and External Network	Must have				
x.*	The solution should be capable of natively integrating with third party security software's like, Palo Alto, Checkpoint, Trend Micro, Fortinet, etc.	Must have				
xi.*	Micro Segmentation of application (VMs) with security policies enforced at each individual VMs	Must have				

xii.*	The solution should integrate with existing network monitoring tool which supports SNMPv2, SNMPv3.	Must have				
xiii.	The HCI solution should provide L4-L7 load balancer with server health checks, and rules for programmability and traffic manipulation. The following is the minimum required features: Load Balancing: UDP, TCP, HTTP, HTTPS (SSL offload, pass-through, end to end), FTP Methods: Round Robin, Source IP hash, Least Connection, URI/HTTP header/URL. Health Checks: TCP/UDP, HTTP, HTTPs	Must have				
xiv.	There should be logically isolated tenants available with private IP subnet, and are connected by virtualized networks including Virtual Local Area Networks (VLANs) or encrypted channels supporting multiple networks	Must have				
xv.	It should allow bring your own public IP address range (BYOIP) to private cloud.	Must have				
xvi.*	The firewall-rule table of the solution should be designed for ease of use and automation with virtualized objects for simple and reliable policy creation.	Must have				
xvii.*	The solution should have the ability to provide on-demand creation of security groups based on existing security policies.	Must have				
xviii.	The solution should have the ability for On-demand network creation and can define routed, NAT or Private network profiles based on application topology.	Must have				
xix.*	For instance-level protection, Security groups can be used to act as virtual firewalls to restrict traffic for one or more instances.	Must have				
xx.*	For subnet-level protection, access control lists (ACLs) can be used to limit a subnet's inbound and outbound traffic.	Must have				
xxi.*	There should be support of server, storage, network, and database encryption at transit and rest state	Must have				

xxii.*	HCI Software Solution should be STIG compliant or any other such reputed Compliance. Other Certifications can be TAA, FIPS, SP800-53 Guidelines etc.	Must have				
xxiii.	The network manager should be able to manage private networks to interconnect public IP address pools and expose services to the Internet.	Must have				
xxiv.	As different virtual networks can share a common physical link, the network manager should provide an automated procedure for MAC and IP address assignment to avoid address overlap problems.	Must have				
xxv.	Private cloud platform network solution should be scalable and redundant (active – active and active passive clustering).	Must have				
xxvi.	The Solution should have the capability for moving Virtual Machines from Primary site to the Secondary site.	Must have				
xxvii.	Private cloud platform network should provide creation of MZ/DMZ with required security policies.	Nice to have				
xxviii.*	private cloud platform network should have low latency, low jitter, all protocol required to run application (TCP, UDP etc.), network access list and Prevent IP Spoofing features.	Must have				
xxix.*	The proposed solution should provide/integrate with Multi factor authentication.	Must have				
2	**Security Operation**					
i.*	The Solution should provide security on the System OS, as well as guest VMs. As per ReBIT IS policy	Must have				
ii.*	Network and security should be integrated with private cloud so automated and on-demand creation of network, Security and load balancing, SSL VPN policies is done as soon as VM is created.	Nice to have				
iii.*	Virtual Firewall functionality should allow block/allow inbound and outbound traffic to private cloud network, The traffic should be controlled using ACL.	Must have				

iv.*	All Security solutions provided along with HCI layer should work in High availability.	Nice to Have				
v.*	The security solution provided along with HCI layer should able to scan the environment and Guest VMs for any security vulnerability on delivered servers/Systems.	Nice to have				
vi.*	The Solution should be capable to provide agentless guest introspection services like Anti-Malware etc and Network introspection services like IPS/IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for private cloud, container network and security for container to container L3 networking and micro segmentation for micro services etc.	Nice to have				
vii.*	The Solution must offer Policy based administration by putting User Departments Machines (Virtual or Physical) in logical groups and apply relevant policies	Must have				
viii.*	Secure Boot feature must be available for all devices as part of the private cloud infrastructure	Must have				
ix.	The Solution should have mechanism to proactively detect and address potential hardware and software faults during runtime	Nice to have				
x.*	The solution should follow SSDLC (Secure System Development Lifecycle) process and practices as per ReBIT's requirement	Must have				
xi.*	The solution should provide Guest OS templates based on industry standard like CIS benchmark	Must have				
xii.*	The Solution components and VM's should be able to integrate with data leakage prevention (DLP)	Nice to have				
3	**Security Monitoring**					
i.*	Solution should provide visibility, dashboard to collect and analyse network flows in the context of the VMs and applications they are originating from or terminating to. Administrator should easily understand traffic/communication flow.	Must have				

ii.*	Ensure that the private cloud infrastructure and all systems hosted are properly monitored for unauthorized activities.	Must have				
iii.	Solution should monitor resources utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion and The solution should provide network flow monitoring feature.	Must have				
4	**Encryption and Compliance Services**					
i.*	Data encryption applies to the following data on private cloud - Data at rest - Data in motion - Data available over an API to external sources /applications	Must have				
ii.*	Data should be encrypted as per the industry acceptable Encryption Standards and policies	Must have				
5	**SOC-NOC**					
i.*	The private cloud solution should support integration with enterprise security infrastructure and network security infrastructure – SIEM, PIM, Network Monitoring Services	Must have				
ii.*	Network Time Protocol needs to be configured.	Must have				
iii.	All devices proposed should be IPv6 compatible and all licenses should be provided along with hardware.	Must have				
iv.*	None of the device should send any file or data outside Private Cloud network.	Must have				
v.*	The solution should allow authorized administrators, developers or business users to request new IT services and manage specific private cloud and IT resources, while ensuring compliance with business policies	Must have				
D	**Patch Management**					
i.*	The Solution should provide patch management capabilities such that it should be able to update patches on its own hypervisor and update guest operating system.	Must have				

ii.*	Bidder should ensure that compute instances receive OS patching, health checking, Systematic Attack Detection and backup function.	Must have				
iii.*	Solution should have tools/software incorporated to patch all the provisioned VM (Linux & Windows) in private cloud, through automated Patching tool.	Must have				
E	**Audit**					
i.*	Solution should compliant to RA (Risk Assessment) and VAPT (Vulnerability Assessment and Penetration Testing) carried out by ReBIT every six month or as per ReBIT's discretion for the On-Premise private cloud solution. Bidder should take the corrective action against the observations/vulnerabilities and submit the reports at no additional cost.	Must have				
ii.	The bidder should be responsible to provide the documentation and Maintenance of the Policies, Practices and Operating Procedures, Disaster Recovery and Business Continuity Plan for private cloud.	Must have				
iii.*	Provision to provide the audit logs to ReBIT NOC-SOC to identify any unauthorized access to cloud systems. Capability to support storing log files for duration of project in a durable and inexpensive storage solution. This information is useful to improve private cloud security and protect it from threats such as unauthorized access, abusive use of resources, and other forms of intrusion. Auditing provides information about activity in private cloud resources, indicating - who accessed private cloud resources? - when they gained access - what operations they performed	Must have				
iv.	Governance and Compliance: Capability to discover private cloud resources and view the configuration of each. Receive notifications each time a configuration change.	Must have				
F	**Business Continuity**					

i.	Solution must ensure High availability for virtual machines.	Must have				
ii.	Solution must provide replication at appropriate level including virtual machine and storage level within private cloud.	Must have				
iii.	Solution should provide movement of virtual machines from one cluster to another cluster in case of failure or during maintenance work.	Must have				
iv.*	All network and security profiles including IP addresses should remain intact when VMs moves or started within another Cluster or environment.	Must have				
v.	The solution should provide report of every recovery plan workflow executed with details of each and every step like start time, end time, execution status etc.	Must have				
G	**Storage**					
i.	The solution should be All Flash Hyper Converged Appliance- 3 DWPD	Must have				
ii.	– Private cloud software should support storage scalability.	Must have				
iii.	The solution should provide a redundant data caching tier that supports SSD, Ultra DIMM and NVMe	Must have				
iv.	There should be automatic block storage volume attached as a primary boot volume	Must have				
v.	The solution should have the ability to change storage policies applied on VMs on the fly without having to restart workloads.	Must have				
vi.	The solution should also support storage space efficiency features like enterprise class deduplication, compression with erasure coding.	Must have				
vii.	Storage should be integrated with the hypervisor but the upgrades of the hypervisor and SDS should not cause any impact while upgrades.	Must have				
viii.	Solution should provide automatic self-rebalancing feature.	Must have				
ix.	The storage solution with the HCI should have in-built software defined storage capability integrated within the	Nice to have				

	Hypervisor kernel itself or should be using virtual storage controller architecture					
x.	Storage should be based on distributed architecture with data locality of data written to a node.	Must have				
xi.	The proposed solution should have built-in replication capability which will enable efficient array-agnostic replication of virtual machine's data over the LAN.	Must have				
xii.	The solution should provide orchestration layer to have automated disaster recovery.	Must have				
xiii.	Solution should provide QoS capabilities for storage I/O that are enforced across all virtual machines accessing a storage, regardless of which host they are running on either automated or configurable.	Must have				
xiv.	Virtualization software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues.	Must have				
xv.	Storage array should be configured in No-Single-Point-of-Failure configuration with redundant components and offer Five 9's of availability	Must have				
xvi.	Array should be supplied with at least 128 GB Cache on controller pair which should be flexibly usable for Read and write operations. All writes must be mirrored across controllers.	Must have				
xvii.	The array must keep write cache persistent during fault conditions.	Must have				
xviii.	The proposed solution must be configured with usable capacity as per requirement (with no compression & de-duplication) using Raid 6 (6:2), with at least 20% SSD drives. It is desired that no automated tiering should be considered.	Must have				
xix.	The proposed array must field upgradable drives in future to reduce cost. The added SSD/SAS should be	Must have				

	included in existing storage non-disruptively to add capacity.					
xx.	Private cloud infrastructure should support big data computing and should have capability to combine large storage data & multiple network protocols as a single converged infrastructure.	Must have				
xxi.	The Storage array must provide end-to-end data protection using industry standard mechanism such as parity checking, checksum and background disk scrubbing etc.	Must have				
xxii.*	The Storage array must provide multiple levels of access control including role-based security and auditing capability.	Must have				
xxiii.	The storage system should support non-disruptive field replacement capabilities for components like Disk Drives, Disk connections, power supplies, controllers etc.	Must have				
xxiv.	The Storage array should support continuous system monitoring, call-home notification, advanced remote diagnostics and proactive hot sparing to enhance system robustness, availability and reliability.	Must have				
xxv.	The Storage array must support capability to replicate data to remote site array in synchronous and asynchronous modes.	Must have				
xxvi.*	Entire storage capacity should be protected with Data-at-rest encryption, required software and hardware should be configured.	Must have				
xxvii.	The HCI storage controller should support storage array expansion to upgrade higher model	Must have				
xxviii.	The storage should be configured with easy to manage, simple integrated user interface for distributed storage environments.	Must have				
xxix.	Storage should be configured with required feature to snapshot and restore file and block data.	Must have				

xxx.	Storage should provide simple to use single management interface. It should have dashboards for at-a-glance management and reporting and other functions like configuration monitor and manage. It should support any browser and any device/handheld.	Must have				
xxxi.	Storage should support CLI, Web and Rest API based management of storage array.	Must have				
xxxii.	It should have enterprise dashboard to aggregate view of entire storage environment and capability to customize dashboard with IOPS, Throughput, analytics, Storage health reporting and trend analysis. It should have dashboard for alerts on severity to allow instant update on the storage environment for quickly and efficiently detection of issues in real time in order to simplify debugging of hardware faults	Must have				
xxxiii.	All nodes use SSD not only for Caching but also as Capacity tier, ensuring all Virtual machines HOT blocks are serviced from Performance Tier.	Must have				
xxxiv.	The solution should provide ability to provision storage dynamically in different options like SSD, on demand IOPS, File storage, cold storage etc.	Must have				
xxxv.	The solution should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.	Must have				
H	**Firewall Specification**					
1	**General Requirement**					
i.	Firewall should be in High Availability Mode.	Must have				
ii.*	Proposed solution should be Next Generation Firewall with Application Layer Security Controls and Threat Prevention framework	Must have				
iii.	The proposed security solution must be in the Leader's quadrant in the Gartner "Magic Quadrant for Enterprise Network Firewalls" as per the latest available report.	Must have				

iv.*	Solution should have hardened OS for both appliance and management platform	Must have				
v.*	Proposed solution should have Multi-Layer Threat Prevention Suite with following controls embedded: a. Prevention against Malware b. Prevention against Bot & Botnets, c. Prevention against malware hosting URL, Prevention against risky web2.0 apps d. Widgets like anonymizers, TOR, P2P, BitTorrent, etc.	Nice to have				
vi.*	The proposed solution should be able to detect & Prevent the Bot communication with C&C	Must have				
vii.	The proposed solution should have a Multi-tier engine i.e. detect & Prevent Command and Control IP/URL and DNS	Must have				
viii.	Appliance should support for Active – Active connections.	Must have				
ix.*	Bulk blocking IP and URL should be enabled with the help of script or automated method	Nice to have				
2	**Hardware and Interface Requirements**					
i.	Firewall appliance should have Console port and USB Ports.	Must have				
ii.	The platform must be supplied with minimum 8x1G copper & 4x10G SFP+ ports.	Must have				
iii.	The platform should support 40Gbps fibre port for future scalability.	Nice to have				
iv.	Appliance should be rack mountable and support side rails if required	Must have				
v.	Solution should have internal dual power supplies, hard disk and cooling fans on the firewall appliances	Must have				
vi.	The platform should support VLAN tagging (IEEE 802.1q)	Must have				
vii.	The firewall should support ISP link load balancing	Must have				
viii.	The firewall must support stateful active-active load balancing and high availability for redundancy.	Must have				
ix.	Should support redundancy High Availability and Load Sharing.	Must have				

x.	Firewall should support Link Aggregation functionality to group multiple ports as single port.	Nice to have				
xi.	Firewall device should be preloaded with SFP connectors/all pre-requisites	Must have				
xii.	Firewall should provide minimum 32 GB of RAM and scalable minimum 64 GB	Must have				
xiii.	Firewall should be scalable minimum 08x10Gbps, 10x1Gbps	Must have				
3	**Performance Requirements**					
i.	Firewall threat prevention throughput must be minimum of 5 Gbps or higher after enabling all the security features (Firewall, IPS, Antimalware (Antivirus, Antibot), VPN, Application and web control) in production environment. The Next Generation threat prevention throughput shall be measured with all the signatures enabled on all the modules available for threat prevention. Packet Scanning with selected signature shall not be considered for the same. Bidder should furnish the published document for the above clause, in case such published document is not available, bidder should submit letter from their OEM in this regard. Letter of OEM should be signed by their product head of the proposed device	Must have				
ii.	The Firewall must support minimum 50,000 concurrent connections	Must have				
iii.	The Firewall must support minimum 10,000 new connections per second processing.	Must have				
iv.	Appliance should have a capability to support for more than 100 VLAN.	Must have				
4	**Architecture Features**					
i.	The communication between all the components of Firewall System (firewall module, logging & policy management server, and the GUI/WebUI Console) should be encrypted with SSL or PKI.	Must have				
ii.	The proposed solution must be able to support Active/Active configuration with IPv4 & IPv6	Must have				
iii.	The firewall appliance/management server should be able to store	Must have				

	configuration and Logs locally and the Solution should also be capable to take backup of the configuration and logs on periodical intervals.					
iv.*	Firewall should support the authentication protocols RADIUS, LDAP, TACACS, certificate based and token-based authentication	Must have				
v.	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades.	Must have				
vi.	Firewall Appliances should deploy for Active – Active or Active-Passive failover architecture for both Firewall & VPN functions as and when required.	Must have				
vii.	It should support the IPSec VPN for both Site-Site & Remote Access VPN.	Must have				
viii.	Firewall should support IPSEC VPN & Remote VPN failover with multiple ISPs	Must have				
ix.	Firewall should support IPSEC VPN failover irrespective of peer firewall OEM	Must have				
x.	Firewall should have SSL VPN functionality	Must have				
xi.	All SSL VPN and Remote access VPN licenses should not cost additional	Nice to have				
5	**Network Protocols/Standards Support Requirements**					
i.	Firewall Modules should support the deployment in Route as well as Transparent Mode	Must have				
ii.	The Firewall must provide NAT functionality, including dynamic and static NAT translations.	Must have				
iii.	All internet-based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Ms-Exchange	Must have				
iv.*	IPSec VPN should support the Authentication Header Protocols – SHA256, AES 256	Must have				
v.*	IPSec ISAKMP methods should support Diffie-Hellman Group 1,2,5,14 & 19, MD5 & SHA Hash, RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange	Must have				

	Material and algorithms like RSA-1024 / 1536 or higher					
vi.*	IPSec encryption should be supported with 3DES, AES-128 & AES-256 standards or higher	Must have				
vii.	IPSec should have the functionality of PFS and NAT-T	Must have				
viii.	It should support BGP, OSPF, RIPv1 &2, Multicast Tunnels, Multicast protocols like DVMRP, PIM etc.	Nice to have				
6	**Firewall Filtering Requirements**					
i.	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports	Must have				
ii.	The Firewall must provide state engine support for all common protocols of the TCP/IP stack	Must have				
iii.*	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type	Must have				
iv.*	It should support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP and Skinny flows.	Nice to have				
v.	It should support CLI & GUI based access to the firewall modules	Must have				
vi.	QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits and QOS VPN]	Must have				
vii.	Firewall should support FQDN filtering and policy creation	Must have				
7	**Integrated IPS Feature Set**					
i.*	Integrated IPS functionality should be available as a software module that can be activated and de-activated as and when required.	Must have				
ii.*	The IPS should be constantly updated its database for defences against emerging threats.	Must have				
iii.*	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time.	Must have				

iv.*	Should have flexibility to define signatures in detect or prevent or both modes as per organization requirement.	Must have				
v.*	IPS Engine should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour-based detection.	Must have				
vi.*	Intrusion Prevention should have option to add exceptions for network and services.	Must have				
vii.*	IPS should have the functionality of Geo Protection to Block the traffic country wise and connection wise (Outbound/inbound)	Must have				
viii.*	IPS events/protection exclusion rules can be created and view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for the analysis.	Nice to have				
ix.*	IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc	Must have				
8	**Content/URL Filtering/UTM**					
i.*	Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc.	Must have				
ii.*	Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance.	Nice to have				
iii.*	It should be able to block Instant Messaging like Yahoo, MSN, ICQ, telegram, Skype (SSL and HTTP tunnelled)	Nice to have				
iv.*	It should enable blocking of Peer-Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP)	Must have				
v.*	Solution should have application control, URL filtering, categorization	Must have				
vi.*	Solution should provide DDOS protection	Must have				
9	**Identity Awareness Features**					

i.*	Firewall Should support Identity Access for Granular user, group and machine-based visibility and policy enforcement.	Must have				
ii.	Firewall should support the Identity based logging.	Must have				
iii.	Should provide seamless AD Integration with multiple deployment options like Clientless, Captive Portal or Identity Agent.	Must have				
iv.	Identity awareness licensing should not be restricted on the basis on users.	Must have				
10	**Administration, Management, & Logging / Reporting Functionality**					
i.	For firewall Real-Time Monitoring, Management & Log Collection, OEM should provide external log storage device.	Must have				
ii.	DC Firewalls should be manageable either from on-device management or from centralised management framework. In case if device doesn't have on-device management, vendor need to provide central management.	Must have				
iii.*	Any changes or commands issued by an authenticated user should be logged to a database.	Must have				
iv.	Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter.	Must have				
v.	Firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes.	Must have				
vi.	The Firewall administration station must provide a means for exporting the firewall rules set and configuration.	Nice to have				
vii.*	Support for role-based administration of firewall.	Must have				
viii.	The Firewall administration software must provide a means of viewing, filtering and managing the log data.	Must have				
ix.	The Firewall logs must contain information about the firewall policy rule that triggered the log.	Must have				

x.	The Firewall must provide a minimum basic statistic about the health of the firewall and the amount of traffic traversing the firewall.	Must have				
xi.	Management should provide detailed Event analysis for Firewall, IPS, Application Control, Data filtering with reporting of all the components.	Must have				
xii.	External log storage device capacity should be minimum 1TB and it should be scalable up to 5 TB.	Must have				
11	**Sandboxing**					
i.*	Solution should detect and block new, unknown malware and targeted attacks found in email attachments, downloaded files, and URLs to files within emails	Must have				
ii.*	Solution should provide protection across one of the widest ranges of file types including, MS Office, Adobe PDF, Java, Flash, executables, and archives, as well as multiple Windows OS environments	Must have				
iii.*	Solution should inspect threats hidden in SSL and TLS encrypted communications	Nice to have				
iv.*	Solution should provide complete reports for file analysed and their status	Must have				
v.	All above device should support integration with SIEM for Log co-relation	Must have				
J	**Virtualization**					
i.	Virtualization software should provide a virtualization layer that sits directly on the bare metal server hardware	Must have				
ii.	Hypervisor layer should provide High Availability for VMs/ DRS and equivalent features.	Must have				
iii.	Hypervisor layer should support live migration of running virtual machines from one physical node to another with zero downtime, continuous service availability, and complete transaction integrity transparent to users and balancing of available resources with rules to define affinity and/or anti affinity for workloads.	Must have				

iv.	The virtualization management software should have the ability to live migrate VM files from one storage array to another with minimum downtime for migration from existing storage to new HCI platform.	Must have				
v.	Virtualization software should provide dynamic power management such that in case of during off peak hours not all VMs are required to be powered on due to less load it should place few servers in G2/S5 (Soft Off) power state as per the Industry Standard Advanced Configuration and Power Interface (ACPI) specifications to save power in an automated or manual or scheduled manner	Nice to have				
vi.	The solution should provide network traffic-management controls to allow flexible partitioning of physical NIC bandwidth between different network traffic types and allow user-defined network resource pools, enabling multitenancy deployment	Must have				
vii.	The HCI solution should also store a redundant copy of the data which is accessible immediately by the Hypervisor and application	Must have				
viii.	The solution should provide zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process. This should be via GUI	Must have				
ix.	The proposed solution should be able to inter-operate with another existing ecosystem in the data-center (for e.g. It should be able to inter-operate with traditional FC/ISCSI or even Physical Server storage on other clusters so that the platform is not locked down and siloed into only HCI technology moving forward).	Must have				
x.	The solution should offer VM/ Hypervisor based replication integration to deliver VM-centric, replication that eliminates dependence on storage.	Must have				

xi.*	The solution should support AES-128 and AES-256 encryption (in conjunction with any KMIP 1.1 compliant KMS server) of the workloads when at rest on storage without modifying the Guest OS	Must have				
K	**Management**					
i.	One Click non-disruptive rolling upgrades of Hyper converged system software and system firmware from the same management GUI console	Must have				
ii.	The solution should support Online Analytics on Health of the storage and provide predictive alerts	Nice to have				
iv.	Provide granular VM-Centric controls for managing storage service levels	Must have				
v.	Single dashboard to manage and provision virtual machines, network, security, storage, monitor performance and manage events & alerts	Must have				
vi.	The solution should provide prebuilt & customizable operations dashboards & reports to provide real-time insight into infrastructure behaviour, upcoming problems and opportunities for efficiency improvements	Must have				
vii.	The solution should provide assistance in troubleshooting and operational management in the virtualized environment	Nice to have				
viii.	The solution should provide a log analytical tool which will collect data from various data Sources limited to HCI	Nice to have				
ix.	The solution should pre-emptively rebalance workloads in advance of upcoming demands and spikes, eliminating resource contention before it happens thus ensuring that workloads get the resources that they always need.	Must have				
x.	The VM manager is responsible for managing a VM's entire life cycle and performing different VM actions- - Deploy - Migrate - Suspend - Resume - Shut down	Must have				

	This should be in accordance to user commands or scheduling strategies and it should be able to report VM availability in private cloud infrastructure to guarantee VM availability, the VM manager should include different mechanisms for detecting VM crashes and automatically restarting the VM in case of failure					
L	**OEM**					
i.	Direct OEM 24x7x365 days Business Critical support for all the components with unlimited incident support (Telephonic/Web) including the unlimited upgrades and updates for 5 years	Must have				
M	**Operations Management Technical Specifications**					
i.	The solution should provide unified management of performance and capacity for the proposed platform via a role-based web interface	Must have				
ii.	The solution should provide the ability to identify and report on over-sized, undersized, idle and powered-off virtual machine such that the environment can be right-sized, and resources can be reclaimed	Must have				
iii.	The solution should provide predictive analytics capabilities to understand baselines and model capacity and demand for accurate forecasting of infrastructure requirements	Nice to have				
iv.	The solution should provide configuration compliance reports/alerts/dashboards for the underlying hypervisor platform	Must have				
N	**Other**					
i.*	Infrastructure should be SOC Ready and Security Compliant. Should have Business Continuity Process (BCP) Ready w.r.t. regions, zones, etc.	Must have				
ii.*	It should provide quick instance provisioning with high network performance - Stock images or custom images that can be imported from another Object Storage	Must have				

	- All images should be cloud-init enabled - It should manage large number of images efficiently and securely - Virtual instances be connected without using a password by adding SSH keys - Adequate network bandwidth per instance to be created - Virtual instance should be multi-homed and capable of multiple network interfaces per instance to be created					
iii.	**Data Locality:** Maintain primary working set copy of active data on the Local node where VMs are being hosted (Data and I/O locality), in order to provide high IOPS and low latency.	Must have				
iv.	**Data Tiering:** Block Level Support for real-time data storage tiering between SSD and HDD disks to maintain optimal performance should be a part of the solution and any licenses for the same should be incorporated as part of the proposal.	Must have				
v.	**File Services:** The proposed HCI must natively support File Services (NFS, CIFS & SMB) without use of 3rd party tools and file replication across HCI clusters and data centres.	Must have				
vi.	**Resiliency:** The HCI platform should have ability to replicate VM's independently & irrespective of the Hypervisor Software. The proposed solution must support ability to do a 2-way & 3-Way Replication (Sync & Async) and be capable of providing Zero data loss solution.	Must have				
vii.	**Scalability:** HCI solution should support dynamic scalability without Zero downtime and automated resource allocation during upgrades. The upgrade should be granular and in 1 node increments. The solution must support adding storage only nodes if needed without resulting in additional SW license cost either for DBs or hypervisor.	Must have				

viii.	**Interoperability:** Proposed HCI solution should support mix and match various node configurations and Intel CPU generations in the same cluster. This will allow customer flexibility to use advancement in CPU technology without any limitations.	Must have				
ix.	The proposed solution must have capability to integrate with leading public cloud service providers.	Must have				
x.	The proposed solution should provide seamless upgrade for Firmware, Hypervisor, Storage OS, BIOS and other such functions which are required in the HCI platform. The upgrade should be online and should not mandate any kind of OEM engagement.	Must have				
xi.	Hypervisor should provide the ability to hot add vCPU and memory, hot-plug disks and NICs (provided the same is supported by guest OS.).	Must have				
xii.	Hypervisor should provide ability to grant / ensure resources to virtual machines as they need for hosting latency sensitive workloads. Also, the initial placement of workloads should consider CPU, Memory and Storage contentions / hotspots.	Must have				
xiii.	Hypervisor should have ability to expand boot and non-boot disks without downtime and providing options for locating new virtual disks for existing workloads on different tiers of storage for Windows, Linux etc. workloads.	Must have				
xiv.	Hypervisor should have I/O prioritization for virtual workloads to ensure business critical VM's are not affected due to congestion of other VM's on the same host.	Must have				
xv.	Hypervisor should provide zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.	Must have				
xvi.	Hypervisor should provide centralized disk-based protection (backup/restore) capabilities for the virtual Windows, Linux etc. workloads with file level	Must have				

	restore and built-in de-duplication to reduce backup storage requirements.					
xvii.	Solution should support configurations of 802.1q VLAN's which are compatible with standard VLAN implementation of other vendors.	Must have				
xviii.*	Other Managed Services - OS Management - DB Management - Security Management - Network Management - Real Time Latency Monitoring Tool - DDoS Protected Bandwidth - Real Time Monitoring of Bandwidth Usage - Multilayer Configuration of Devices - Network Governance - Monitoring Management - Monitor more parameters - Deep Monitoring including Services - SMS and Email alerts for Instant Action -Automated Ticket Generation and Proactive Resolution - Content Delivery Network (CDN) for App, Web - External Object Storage like AWS/S3 - Disaster Recovery of Cold DR with Backup (Active-Passive model) - Hardware or Software Key Management Systems (KMS).	Must have				
O	**Private cloud tools and applications**					
1	**Administrative tools**					
i.	The portal should provide one stop, online access to the product, a personalized dashboard to monitor device health, hardware events, and contract and warranty status. Should provide a visual status of individual devices and device groups.	Must have				
2	**Scheduling tools**					

i.	The Private cloud solution should be capable of scheduling jobs at the physical host level which is responsible to decide when VMs can obtain system resources such as physical CPU, memory.	Must have				
3	**Private Cloud Interfaces**					
P	**Replication software**					
i.	The proposed replication software must provide the ability to perform synchronous as well as asynchronous replication in the virtualized machine environment over any distance with efficient WAN bandwidth utilization.	Must have				
ii.*	The proposed replication software must support continuous data protection to any point in time recovery at the virtual machine level and it must provide inbuilt ability to perform DR orchestration workflows.	Must have				
iii.	The proposed solution should run on dedicated clustered configurations to avoid single point of failure and must support scale up configuration by adding additional appliances.	Must have				
iv.	It must support replication of virtual disk as well as Raw device mappings (RDM) disks within a virtual machine.	Must have				
v.	It must support flexible deployment models by using virtual appliances and virtual disks for its journaling volumes. The architecture of the solution must have no single point of failure.	Must have				
vi.	It must provide REST API's to enable deployment workflow automation.	Nice to have				
vii.	It must support automatic provisioning of target VM's as well as the journals.	Must have				
viii.	It must provide the flexibility to exclude virtual disks within the protected VM from the replication configuration.	Must have				
ix.	The proposed software must provide the ability to perform DR tests without failing over the Production volumes. During the drills/test the Production volumes must continue replicating to the replication target and any operation on the source VM/volume must remain unaffected.	Must have				

x.	The software must be able to failover an individual or group or complete site to another site.	Must have				
xi.	The proposed software must support defining of the power up sequence during a fail over process.	Must have				
xii.	Proposed Replication Solution should be able to Replicate to Traditional/Converge Infrastructure as well if required.	Nice to have				
Q	**Core Switch**					
1	**OEM Capabilities**					
i.	The OEM suggested should be a part of the Leaders quadrant of (latest Gartner Report) Magic Quadrant for Wired Infrastructure	Must have				
2	**Switch Physical Capabilities**					
i.	The proposed solution must be a purpose built 1RU rack-mountable appliance.	Must have				
ii.	The Switch should have N+1 redundant Power Supplies. Power Supplies should able to cater the need of quoted switch when it is fully populated.	Must have				
3	**Port Requirements**					
i.	Minimum non-blocking 12 X 10GE Copper ports (with stacking) fully loaded as per pre-requisites	Must have				
ii.	Minimum non-blocking 12 X 1/10GE SFP ports (with stacking) fully loaded SFP connector	Must have				
iii.	Should provide minimum Switching Capacity of 320Gbps	Must have				
iv.	Should provide minimum throughput of 250 Mpps	Must have				
v.	The switch should support all standard protocols (i.e. OSPF, BGP etc.)	Must have				
vi.	The switch should support minimum 4000 active VLANs	Must have				
vii.	Switch shall support IPv4 & IPv6	Must have				
4	**Layer 2 and Layer 3 Switch features**					
i.	Traffic Marking: IEEE 802.1Q/P, ACLs	Must have				

ii.	Congestion Avoidance	Must have				
iii.	Mechanism to detect connectivity issues with fiber. Ensure that partially failed link is shutdown on both sides, to avoid L2/L3 protocol convergence issues.	Must have				
iv.	Should support Port Mirroring based on acl, port basis / vlan basis to support intrusion prevention system deployment in different VLANs. Should support port mirroring across the stack switches to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.	Must have				
v.	Switch should provide minimum 2 or more mirror sessions	Must have				
vi.	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.	Must have				
5	**High Availability Features**					
i.	The switches in stack/HA should support Stateful Switchover	Must have				
ii.	The stacking/HA connectivity should be via dedicated stacking modules	Must have				
6	**QoS Features**					
i.	Enterprise wide QoS Management (LAN, WAN Integration)	Nice to have				
ii.	Quality of Service with minimum 8 queues per port.	Nice to have				
iii.	Micro-Flow Policing (BW limiting on user/application)	Nice to have				
iv.	Strict Priority Queue (Protection of Mission critical traffic, delay sensitive traffic)	Nice to have				
v.	Aggregate Flow Policing (Dedicated BW per customer)	Nice to have				
vi.	Scheduling IP precedence, 802.1p priority, three transmit queues on a per port basis, WRR, Strict Priority Queue TOS<->COS mapping	Nice to have				
7	**Software based standards for Network Device**					
i.	RMON capabilities.	Must have				

ii.	The switch should provide 802.1x based authentication protocol for posture assessment.	Must have				
8	**Management Features**					
i.	Switch must support Secure Shell Version2 (SSHv2), Telnet & SNMPv2, and SNMPv3.	Must have				
ii.	Switch must have single console port for Command-Line Interface (CLI) management	Must have				
iii.	Switch must support time synchronization via SNTPv4	Must have				
iv.	Switch must support IEEE 802.1AE	Must have				
v.	Switch must support integration with SIEM on standard port	Must have				
9	**Troubleshooting Capabilities**					
i.	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.	Nice to have				
ii.	Switch should generate hardware failure information in a log file and need to be stored in flash so that support center can access these files and to identify the root cause	Must have				
10	**Security Requirements**					
i.*	It should support port security to secure the ports against mac floods and unaccounted accesses	Must have				
ii.*	It should support protected ports to isolate specified ports from all other ports on the switch.	Must have				
iii.*	Switch Should support VLAN Based and Port Based ACLs	Must have				
iv.*	Switch should provide 802.1x support for VLAN assignment, port security and ACL support	Must have				
v.*	It should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address.	Must have				
vi.*	It should support TACACS+ or RADIUS authentication for secure switch CLI logon.	Must have				
vii.*	It should support management access (CLI, Web, MIB) securely encrypted	Must have				

	through SSHv2, SSL, SNMPv2 and SNMPv3.					
viii.*	Per-port storm control for preventing broadcast, multicast, and unicast storms	Must have				
ix.*	The switch should support monitoring, capturing, and recording of flows to provide network traffic statistics for further analysis, accounting, network monitoring and network planning. Flows need to be captured from physical Ethernet port or from vlan interface.	Must have				
R	**Server Switch**					
1	**OEM Capabilities**					
i.	The OEM suggested should be a part of the Leaders quadrant of Magic Quadrant for Wired Infrastructure as per the latest available report.	Must have				
2	**Switch Hardware Features**					
i.	Minimum 48 10Gbps port each. fully loaded as per pre-requisites hardware (ethernet, fiber, SFP connector)	Must have				
ii.	Switch should be rack mountable in nature, stackable with dedicated 40Gbps of throughput with minimum of 4 switches in a stack with single IP management.	Must have				
iii.	Should provide minimum Switching Capacity of 320 Gbps	Must have				
iv.	Should provide minimum throughput of 250 Mpps	Must have				
v.	The Switch should have N+1 redundant Power Supplies. Power Supplies should able to cater the need of quoted switch when it is fully populated.	Must have				
3	**Layer 2 Requirements**					
i.	The switch should support full Layer-2 services	Must have				
ii.	The switch should support minimum 500 active VLANs	Must have				
iii.	The Switch should provide full Multicast capabilities.	Must have				
iv.	The Switch should provide port security	Must have				

v.	The switch should provide 802.1x based authentication protocol for posture assessment.	Must have				
vi.	Should support Port Mirroring based on acl, port basis / vlan basis to support intrusion prevention system deployment in different VLANs. Should support port mirroring across the stack switches to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.	Must have				
vii.	Switch should provide minimum 2 or more mirror sessions	Must have				
viii.	Switches should be stackable	Must have				
4	**Management Requirements**					
i.	Switch can be managed with SSHv2, SNMPv2 and SNMPv3	Must have				
ii.	Switch shall support IPv4 & IPv6	Must have				
iii.	Should support minimum 2 X 1 GE uplink port and 4 X 10 GE uplink ports	Must have				
iv.	Should have stacking capacity up to 3X of minimum switching capacity.	Must have				
v.	Switch must support time synchronization via SNTPv4	Must have				
vi.	Switch must have single console port for Command-Line Interface (CLI) management	Must have				
5	**Security Requirements**					
i.*	It should support port security to secure the ports against mac floods and unaccounted accesses	Must have				
ii.*	It should support protected ports to isolate specified ports from all other ports on the switch.	Must have				
iii.*	Switch Should support VLAN Based and Port Based ACLs	Must have				
iv.*	Switch should provide 802.1x support for VLAN assignment, Guest VLAN, MAC-AUTH Bypass and ACL support	Must have				
v.*	It should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client's MAC address.	Must have				
vi.*	It should support TACACS+ or RADIUS authentication for secure switch CLI logon.	Must have				

vii.*	It should support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, SNMPv2 and SNMPv3.	Must have				
viii.*	Per-port storm control for preventing broadcast, multicast, and unicast storms	Must have				
ix.*	The switch should support monitoring, capturing, and recording of flows to provide network traffic statistics for further analysis, accounting, network monitoring and network planning. Flows need to be captured from physical ethernet port or from vlan interface.	Must have				
6	**QoS Requirements**					
i.	It should support IEEE 802.1p traffic prioritization delivering data to devices based on the priority and type of traffic.	Must have				
ii.	should have strict priority queuing or high strict priority queue	Must have				
7	**Troubleshooting Requirements**					
i.	Switch should support Layer 2 traceroute to identify the physical path that a packet takes from source to destination	Nice to have				
ii.	Switch should generate hardware failure information in a log file and need to be stored in flash so that support centre can access these files and to identify the root cause	Must have				
S	**Link Load Balancer**					
i.	Link Load Balancer should have minimum 6 * 1G interfaces.	Must have				
ii.	Link Load Balancer should support minimum 2 x 200 Mbps internet bandwidth in active-active mode and active standby failover mode.	Must have				
iii.	It should be intelligent to handle multiple links of different capacity and able to utilize the same accordingly.	Must have				
iv.	It should support dynamic redirecting of traffic via the best performing link.	Must have				
v.	It should support setting a priority for each type of traffic	Nice to have				
vi.	It should support Geolocation and Proximity based load balancing	Nice to have				

vii.	Should support Static NAT, Port based NAT and advanced NAT for transparent use of multiple WAN / Internet links.	Nice to have				
viii.*	The proposed appliance should provide integrated functionalities of Link Load Balancer, DNS and L3-L4, DNS DDOS	Must have				
ix.	The proposed solution should provide throughput of 10 Gbps	Must have				
x.	Should have minimum DNS QPS of 1000 from day one and upgradable to 325,000 with license upgrade	Must have				
xi.	In case of link failure, device should detect it in less than 30 seconds and divert the traffic to other available links.	Must have				
xii.	Shall provide individual link health check based on physical port, ICMP Protocols, user defined ports and destination path health checks.	Must have				
xiii.	Should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation.	Nice to have				
xiv.*	The Solution should be able to prevent DNS flooding attack.	Must have				
xv.*	The Solution should be able to effectively mitigate DNS nxdomain flooding attack.	Must have				
xvi.*	The solution should support Dynamic IP Shunning, BGP Blackholing and auto tuning of the DOS thresholds	Must have				
xvii.*	Proposed solution should be manageable from a single management platform	Must have				
xviii.*	Should Support integration with SIEM and other Monitoring and Reporting solution	Must have				
xix.	The proposed OEM should have direct presence in India and should have a registered office in India	Must have				
xx.	Solution should support HA	Must have				
xxi.	The OEM should be in the Gartner's Leaders Magic Quadrant for "Application Delivery Controllers" in the latest published report.	Must have				

T	Server/Application Load Balancer					
i.	The proposed appliance should provide integrated functionalities of server load balancer, SSL.	Must have				
ii.	The proposed appliance must provide minimum 4 x 1G ports and 4 x 10G SFP+ ports (It should be fully loaded with all pre-requisite)	Must have				
iii.	The proposed appliance should provide minimum throughput of 5 Gbps	Must have				
iv.*	The proposed appliance must support minimum SSL TPS of 2000, scalable to 4000 with RSA 2048-bit keys and minimum SSL TPS of 1700, scalable to 3400 with ECDSA P-256-bit keys	Must have				
v.	The proposed appliance should support minimum 4 Gbps of compression throughput scalable to 5 Gbps	Must have				
vi.	The proposed appliance should support minimum 4 Gbps of SSL throughput scalable to 5 Gbps	Must have				
vii.*	Must be hardware appliance with hardened OS	Must have				
viii.	Should have a dedicated management port	Must have				
ix.	Solution should support Multi VLAN network topology.	Must have				
x.	Should support minimum memory 4 GB scalable up to 12 GB+	Must have				
xi.	Should have an HDD thin provisioning	Nice to have				
xii.	Should have capability to support up to 50000 Concurrent Connections scalable to 1Lacs Concurrent Connections	Must have				
xiii.*	The proposed solution must be able to perform TCP multiplexing and TCP optimization, SSL Offloading with SSL session mirroring and persistence mirroring, hardware-based compression, caching etc. in active-passive mode.	Must have				
xiv.*	The proposed solution must offer out of band programming for control plane along with data plane scripting for functional like	Must have				

	content inspection and traffic management					
xv.	Server Load Balancer should support SQL-based querying for the following databases for health checks: · Oracle · MSSQL · MySQL · PostgreSQL · DB2	Nice to have				
xvi.*	Proposed solution should provide SSL offloading with the SSL connection and persistence mirroring during the HA failover for all connections which are offloaded on the device so that existing SSL connections are not lost during a failover event	Must have				
xvii.*	The proposed appliance should support centralized Security policies enforcement, SSL Certificates management for workloads on Private DC and public cloud	Must have				
xviii.*	The solution must support Constrained Certificate delegation which will allow the device to generate SSL certificates on behalf of the application servers which then can be used to authenticate clients for which SSL certificate based authentication has been enabled.	Must have				
xix.*	Device should support File Upload Violation & scanning for malicious content in Uploads through ICAP integration	Nice to have				
xx.*	The proposed solution must support policy nesting at layer4 and layer7 to address the complex application integration. Further it should also provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..	Nice to have				
xxi.*	Load balancer should support integration with WAF for future enhancement.	Must have				
xxii.	Proposed solution should be manageable from a single management platform	Must have				

xxiii.*	Should Support integration with SIEM and other Monitoring and Reporting solution	Must have				
xxiv.*	The proposed solution should have a feature to generate device snapshot reports which then should be uploaded to an OEM provided online tool and get feedback on the health of the unit & missing Hotfixes and best practices	Must have				
xxv.*	Solution should support Multi-Factor authentication	Must have				
xxvi.	The OEM should be in the Gartner's Leaders Magic Quadrant for "Application Delivery Controllers" and "Web Application Firewall" in the latest published report	Must have				
U	**Backup**					
i.	Backups of all the data including but not limited to files, folders, images, system state, databases, workstations and enterprise applications should be carried according to the following policy- - An initial full backup - Daily incremental with 7 days retention - Weekly full backups with 5 weeks retention - Monthly full backup with 3 months retention - 1 yearly full backup The Bidder should provide optimal sizing for the backup storage based on the size of the private cloud and backup policy provided.	Must have				
ii.	Backup feature should provide GUI based centralized management for all backup activities across the entire storage capacity supplied.	Must have				
iii.	Backup feature should provide de-duplication and compression.	Must have				
iv.	Backup feature should be able to schedule backup and restoration operations.	Must have				
v.	ReBIT envisaged private cloud should be able to integrate with an archival solution later.	Nice to have				
vi.	The solution must support client-direct backup feature for file system,	Nice to have				

	applications and databases to reduce extra hop for backup data at backup/media server to cater stringent backup window					
vii.	Backup feature should support multi tenancy feature for creation of distinct data zones or tenant where the end users have access without being able to view data, backups, recoveries, or modify in other data zones or tenant	Nice to have				
viii.	Backup feature should also have configurable Restful API support for management, administration and reporting on backup infrastructure via custom applications.	Nice to have				
ix.	The proposed backup feature should support restore a single VM, single file from a VM, a VMDK restore from the same management console for ease of use.	Must have				
x.	The proposed backup feature should have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats.	Must have				
xi.	The proposed backup feature should provide search capability from a web portal to allow search for a single file from complete backup store.	Must have				
xii.*	The backup software should be able to encrypt the backed-up data using industry standard encryption.	Nice to have				

Place:

Date:

Authorized Signatory:

Name & Designation:

Business Address & email id: